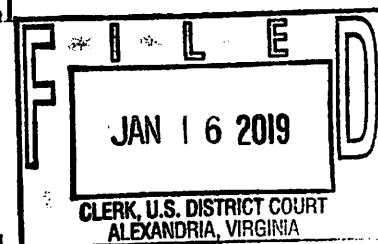


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



Case No.1:19-sw-31

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
42838 Falling Leaf Court, Ashburn, Virginia 20148, which
is a multi-level single family house with a two-car attached
garage

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1832	Theft of Trade Secrets

The application is based on these facts:
See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Carina A. Cuellar

Austin I. Price

Applicant's signature

Austin I. Price, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 01/16/2019

/s/ *JFA*
John F. Anderson
United States Magistrate Judge
Judge's signature

City and state: Alexandria, VA

Hon. John F. Anderson, US Magistrate Judge

Printed name and title

ATTACHMENT A

The property to be searched is the residence located at 42838 Falling Leaf Court, Ashburn, Virginia 20148. The SUBJECT PREMISES is further depicted in the below photographs and is described as a large single family home on Falling Leaf Court with the numbers "42838" clearly affixed to the home/mailbox and visible from the street. The vehicle has been observed at the SUBJECT PREMISES as recently as January 2, 2019. In addition, the search shall be extended to any locked safe or container within the SUBJECT PREMISES. It shall also be extended to Maros Kmec's Lexus SUV, which he drove to and from work on October 17, 2018.



Google Maps overhead image of 42838 Falling Leaf Court, Ashburn, Virginia 20148

ATTACHMENT B

The following is a list of property to be seized from within the premises known as 42838 Falling Leaf Court, Ashburn, Virginia 20148, a Lexus SUV, and any safes, lockers and closed containers therein, which constitutes evidence, fruits or instrumentalities of violations of the following federal statutes: Title 18, United States Code, Section 1832 (Theft of Trade Secrets); Title 18, United States Code, Section 2314 (Interstate Transportation of Stolen Property); Title 18, United States Code, Section 1343 (Wire Fraud); Title 18, United States Code, Section 2 (Aiding and Abetting the foregoing offenses); and Title 18, United States Code, Section 371 (Conspiracy to commit the foregoing offenses).

- a) Any and all financial, business, scientific, technical, economic and engineering information, of any form or type, relating to ADSI's or another company's proprietary information or trade secrets, which appears to be legally or equitably owned by, or licensed to, ADSI or another company, including, but not limited, to patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs and codes, and contracts, stored in any manner such as physically, electronically, graphically, photographically or in writing.
- b) Any other confidential information related to ADSI's and any other company's proprietary information or trade secrets, including but not limited to business records which reflect the source, development, marketing or sale of proprietary information or trade secret data, including, but not limited to, customer lists, customer files, customer correspondence, customer billing records, pick-up and delivery tickets, employee and drivers records, insurance

records, financial records, invoices, contracts, bank records, investment records, canceled checks, drafts, money orders, cash, memoranda, correspondence, handwritten notes, notebooks, telephone directories, address listings, and calendars.

- c) Any and all records of measures taken to keep secret proprietary information or trade secret data, including but not limited to exit interviews, confidentiality agreements (e.g., with employees, vendors, customers and competitors), non-compete agreements, employee contracts, employee handbooks or manuals, non-disclosure and unauthorized use warnings.
- d) Any and all records of legal or equitable ownership of, or license in, proprietary information or trade secret data by ADSI or any other company, and use or intended use of proprietary or trade secret data.
- e) Any and all records or other materials relating to the theft, misappropriation, unauthorized conversion, receipt, purchase or possession by any person[s] or entit[ies] other than ADSI of the proprietary information or trade secret data including, but not limited to, documents relating to the formation of corporate entities, business plans and venture capital proposals.
- f) Any and all records of employment offers and/or negotiation of employment terms by such person[s] or entit[ies].
- g) Any communications between such person[s] or entit[ies] and parties other than ADSI relating to proprietary information or trade secret data.
- h) Resource or reference materials relating to such financial, business, scientific, technical, economic and engineering information, including, but not limited

to, technical manuals, trade association documents, treatises.

- i) Conversations, whether through text message or other applications, where Maros Kmec discusses ADSI's proprietary information or trade secret data with other individuals.
- j) Computers and associated devices which could be used to transmit or store any of the above described financial, business, scientific, technical, economic and engineering information and books and records, including but not limited to:

- Computer Hardware – all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data, including any data-processing devices (such as central processing units, memory typewriters, self-contained “laptop” or “notebook” computers, mobile phones, including “smart” phones, tablets, and server computers), internal and peripheral storage devices (such as fixed disks, external hard disks/drives, including but not limited to, the Seagate external hard drive discussed in the affidavit, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices), peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers), related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling

devices, and electronic tone-generating devices), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks);

- Digital Storage Devices – any and all tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, including external hard drives, monitors, computer printers, modems, tape drives, thumb drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, tape systems and hard drive and other computer related operation equipment, in addition to computer photographs, Graphic Interchange formats and/or photographs, slides or other visual depictions of such Graphic Interchange format equipment which may be, or are used to send, receive, or store documents in an electronic format;
- Computer Software – digital information that can be interpreted by a computer and any of its related components to direct the way it works, stored in electronic, magnetic, optical, or other digital form, including but not limited to programs to run operating systems and applications (like word-processing, graphics, or spreadsheet programs, utilities, compilers, interpreters, and communications programs);
- Computer-related Documentation – written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, software, or other related items; and

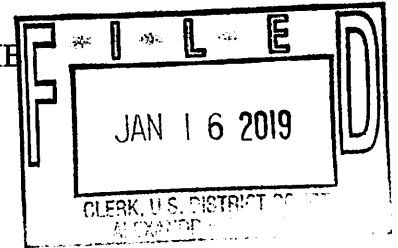
- Computer Passwords and Other Data Security Devices – passwords (usually but not always a string of alpha-numeric characters) and other data security devices, including but not limited to encryption devices, chips, and circuit boards, programming code that creates “test” keys or “hot” keys which perform certain pre-set security functions when touched, software or code which encrypts, compresses, hides, or “booby-traps” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

Definitions

As used above, the terms “information,” “records,” “materials” and “documents” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including floppy diskettes, hard disks and external hard drives, ZIP disks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, mobile phones, including “smart phones,” and tablets, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF:

42838 Falling Leaf Court, Ashburn, Virginia
20148, **which is a multi-level single family
house with a two-car attached garage**

Case No. 1:19-sw-31

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Austin I. Price, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for 42838 Falling Leaf Court, Ashburn, Virginia 20148, the home of MAROS KMEC (hereinafter the "SUBJECT PREMISES"). The aforementioned locations to be searched also include any safes, lockers, and closed containers therein, as well as KMEC's Lexus SUV, more particularly described in Attachment A (attached hereto and incorporated herein by reference). As set forth below, there is probable cause to believe that located within the SUBJECT PREMISES, the Lexus SUV, and any safes, lockers and closed containers therein, are evidence, fruits and instrumentalities, more particularly described in Attachment B (attached hereto and incorporated herein by reference), of violations of Title 18, United States Code, Section 1832 (Theft of Trade Secrets).

2. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 2015. Prior to entering the FBI, I served as a state criminal prosecutor and a Judge Advocate in the U.S. Army. During my employment with the FBI, I have conducted and

participated in several investigations involving violations of U.S. laws, including theft of trade secrets, economic espionage, and fraud, among others. I have participated in the execution of several federal search and arrest warrants in such investigations. I have had training in and have observed multiple methods used to smuggle goods and technology out of the United States and commit espionage contrary to laws of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that MAROS KMEC has committed violations of Title 18, United States Code, Section 1832 (Theft of Trade Secrets). There is also probable cause to search the locations described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes as further described in Attachment B.

RELEVANT STATUTES

5. This investigation chiefly concerns theft of trade secrets, a violation of Title 18, United States Code, Section 1832(a), which provides, in pertinent part, that:

Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys,

photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more such persons do any act to effect the object of the conspiracy,

shall be guilty of an offense against the United States.

18 U.S.C. § 1832(a).

6. The statute defines “trade secret” as:

all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing, if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

18 U.S.C. § 1839(3).

7. The statute defines the “owner” of a trade secret as:

the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.

18 U.S.C. § 1839(4).

PROBABLE CAUSE

A. **Background on the Investigation**

8. The FBI is currently investigating KMEC for stealing sensitive trade secrets during the course of his employment with Airbus Defense and Space, Inc. (“ADSI”), a Herndon, Virginia-based subsidiary of Airbus Group Inc. ADSI is a Cleared Defense Contractor (“CDC”) that manufactures fixed and rotary wing aircraft, homeland security systems, public safety communications, defense electronics and avionics, and threat detection systems.

9. According to ADSI, KMEC was employed by ADSI as a Contracts Officer from on or about February 15, 2015, until his resignation on or about October 17, 2018. According to KMEC’s LinkedIn profile, KMEC was previously employed as a Lead Associate at Booz Allen Hamilton, Inc. (“BAH”), another CDC, from in or around April 2008 to in or around February 2015. KMEC’s LinkedIn profile further indicates that he previously worked as a Senior Contracts Administrator at BAE Systems, Inc. from in or around March 2006 to in or around November 2007. KMEC received his Bachelor of Business Administration and Finance from the University of Arizona.

10. According to U.S. Diplomatic Security Service (“DSS”) and U.S. Citizenship and Immigration Service (“USCIS”) records, KMEC was born in or around 1975, in Slovakia and moved to the United States in 1995. He became a naturalized U.S. citizen in or around 1999. He currently possesses a U.S. passport. KMEC claims that he previously renounced his Slovakian citizenship and destroyed his Slovakian passport. As of on or about November 1, 2018, he had a Secret security clearance and Top Secret eligibility.

B. ADSI's Investigation of Trade Secret Theft

11. During the course of this investigation, I reviewed internal ADSI memoranda concerning the events described herein and interviewed ADSI personnel involved in the internal investigation, including the Head of Ethics and Compliance, the Head of Contracts and Procurement, the Chief Information Security Officer and Head of Cyber Security, and human resources ("HR") and information technology ("IT") personnel.

12. On or about October 1, 2018, ADSI's Head of Contracts and Procurement, who was KMEC's direct supervisor, became aware that KMEC had been working on his personal business during work hours and using ADSI resources to do so. The Head of Contracts and Procurement conducted an online search for KMEC's personal business and identified its public website at <https://farclause.com>. According to the KMEC's public LinkedIn page, KMEC is the "CEO" of Farclause/KM-Logix.

13. Concerned that KMEC could be using ADSI's data to benefit his personal business, ADSI initiated an internal investigation to determine the exact nature and extent of KMEC's use of ADSI resources. ADSI also began to monitor KMEC's network activity. On or about October 15, 2018, ADSI IT personnel determined that KMEC visited the domain farclause.com approximately 8,000 times and downloaded or uploaded approximately 24 megabytes (MB) to or from the website during the preceding ninety days.

14. IT personnel also detected that KMEC had connected an external hard drive to his work-issued laptop for extended periods of time. IT personnel remotely analyzed¹ this hard drive

¹ Company employees are notified, per ADSI's policy, that any information accessed, viewed, or stored on the network may be monitored and recorded and that possible evidence of a violation of crime might be provided to law enforcement.

and determined that it was manufactured by Seagate, contained approximately 650 GB of data, and its serial number was “000001A6 ACF2:6EC1” (hereinafter “the Seagate drive”). The Seagate drive was not ADSI’s property. According to ADSI, KMEC did not have permission to insert the personal hard drive into his work laptop or to download ADSI information, both of which constitute violations of ADSI’s network Acceptable Usage Policy. Among other things, the Acceptable Usage Policy provides that “[w]ithout exceptional circumstances, business data should be stored on the network shared drives . . . and not on a personal hard drive.”

15. ADSI IT personnel determined that an entire folder stored on the Seagate drive was titled “Airbus.” IT personnel remotely imaged (*i.e.*, copied from the hard drive) approximately 78 gigabytes (GBs) of the Seagate drive’s data on October 5, 2018, and approximately 137 GBs of the Seagate drive’s data on October 11, 2018, although the second attempt resulted in data that was partially duplicative of the first.

16. Over the course of the next week, IT personnel continued to remotely monitor KMEC’s network usage; however, they were unable to image the entirety of the Seagate drive and estimated it would take approximately ten consecutive and uninterrupted hours to image the entire 650 GB of data contained on the Seagate drive, given the slow transfer process. ADSI personnel were unable to complete the transfer because KMEC removed the Seagate drive from the laptop when he left ADSI at the end of the day and, at on least one occasion, when he left his office for breaks during the day.

17. ADSI personnel performed a preliminary analysis of a portion of the contents of the hard drive data and concluded that it contained ADSI’s proprietary information, including information that was marked “Proprietary,” “Proprietary Rights,” or “Confidential.”

18. On or about October 17, 2018, at approximately 9:52 a.m., ADSI IT personnel confirmed that KMEC again had inserted the Seagate drive into his laptop that morning. At approximately 10:00 a.m., two members of ADSI IT personnel went to KMEC's office and, in order to attempt to inspect his work laptop and the Seagate drive, informed him that IT personnel were alerted that his laptop had a virus. IT personnel requested permission to perform a diagnostic analysis of his work laptop and the Seagate drive. KMEC informed the IT personnel that he would allow them to remove and analyze his work laptop but that he would not permit them to examine his external hard drive because it was his personal property and he was afraid that they would "crash it."

19. The IT personnel reiterated that it was imperative that they conduct an analysis of the Seagate drive, which appeared to contain ADSI's information, adding that it was ADSI's policy to inspect and review data that was brought onto ADSI property and connected to the network. KMEC opened a folder on the hard drive to show the IT personnel the software he was working on, which he said was unrelated to his work at ADSI. The IT personnel were not permitted to examine the remainder of the contents of the Seagate drive. The IT personnel subsequently left KMEC's office and informed ADSI executives, including ADSI's Head of Ethics and Compliance, that KMEC had denied their request to examine his computer and the Seagate drive.

20. ADSI surveillance camera footage revealed that within minutes of the IT personnel leaving his office, KMEC exited his office at approximately 10:32 a.m. Surveillance camera footage revealed that he went to the third floor's elevator bay, descended in an elevator, entered the ADSI parking garage, and finally departed the garage at approximately 10:37 a.m. in his Lexus SUV. At 11:27 a.m., approximately 50 minutes later, surveillance camera footage

showed KMEC driving back into the parking garage in his Lexus SUV and then returning to his office on the third floor.

21. After KMEC returned to his office, ADSI's Head of Ethics and Compliance went to KMEC's office and requested that he permit ADSI personnel to examine the contents of the Seagate drive because ADSI believed it contained the company's intellectual property. KMEC, in what appeared to be an acquiescence, retrieved an external hard drive from his tote bag and gave it to the Head of Ethics and Compliance. The Head of Ethics and Compliance left KMEC's office with the hard drive, and ADSI personnel subsequently plugged the device into a forensic computer to run an analysis.

22. Based on their technical analysis, ADSI personnel determined that the hard drive provided by KMEC was manufactured by Western Digital ("WD"), contained only approximately 3 GB of data, and its serial number was "0000017F 2869:F598." None of these attributes matched the Seagate drive that ADSI IT personnel determined had been connected previously to KMEC's work computer.²

23. At approximately 2:45 p.m, the Head of Ethics and Compliance returned to KMEC's office and confronted him with her belief that KMEC provided a decoy hard drive in an attempt to trick ADSI. KMEC denied giving her the wrong hard drive, adding that he did not know "what a Seagate [was]."

24. The Head of Ethics and Compliance left KMEC's office and requested that the building security summon the Fairfax County Police Department. Shortly thereafter, IT personnel revoked KMEC's access to the ADSI network.

² As described above, ADSI IT personnel determined that the Seagate drive was manufactured by Seagate, contained approximately 650 GB of data, and its serial number was "000001A6 ACF2:6EC1."

25. KMEC departed his office for the day around 3:30 p.m., at which point the Head of Ethics and Compliance confronted him again in the lobby prior to his exit from the building and again asked him to produce the Seagate drive. She also asked KMEC if he had any ADSI property in his possession, which he denied having. KMEC allowed her to search his tote bag, which only contained the WD drive that they had previously been examined and returned to KMEC.

26. KMEC also allowed the Head of Ethics and Compliance to conduct an inspection of KMEC's Lexus SUV in the parking lot. Based on a cursory review of the vehicle, the Head of Ethics and Compliance did not find the Seagate drive. KMEC then departed the premises in his Lexus SUV.

27. On or about October 17, 2018, at approximately 7:00 p.m., KMEC sent his supervisor, the Head of Contracts and Procurement, a resignation email. ADSI HR personnel contacted KMEC later that evening and asked him to bring all ADSI property in his possession to the office by close of business the next day. KMEC also agreed to meet with HR personnel for an exit interview at 10:00 a.m. the next day.

28. On or about October 18, 2018, at approximately 8:30 a.m., KMEC called HR and told them that he left his work-issued cellular phone with security staff at ADSI's front desk. KMEC informed them he would not be attending the exit interview that morning, as previously agreed.

29. IT personnel later determined that KMEC's work-issued cellular phone had been reset to its original factory settings prior to being left with the front desk and therefore no longer contained any user data. ADSI personnel did not instruct KMEC to wipe the phone prior to handing it in, nor did ADSI personnel initiate the reset remotely.

30. ADSI IT personnel located over forty emails that KMEC sent from his ADSI email account to his Gmail account (maroskmec@gmail.com), from around 2015 through October 17, 2018. The emails included ADSI sales contracts, other CDC's contracting documents, Farclause.com documents, and information about disagreements with other ADSI employees, among others. For example, on or about March 31, 2017, KMEC sent from his ADSI email account to his Gmail account an email containing an ADSI sales contract for the sale of C295W Military Transport Aircraft (MTA) and associated services. The sales contract is to be related to KMEC's work for ADSI and contains general terms and conditions for a proposed sale.

31. In or around June 2017, KMEC sent an email message from his ADSI email account to his Gmail account that included an attachment with a screenshot of the desktop of KMEC's work-issued computer. The screenshot—which appears to have been taken to capture KMEC paying a Loudon County traffic fine—also shows a Seagate removable media device connected to the computer. The screenshot of the desktop reveals that the Seagate removal media device contained a folder called "DATABASES" which contained additional folders titled "MANTECH," and "NES," and files titled "ALL AIRBUS CONTRACTS" and "Cayman – MANT."

32. In another email, sent from KMEC's ADSI email address to the Gmail account on or around October 2017, KMEC sent himself an email with the subject "reset" and a Microsoft Word attachment that contains two screen captures: both images show KMEC visiting the KM-Logix website.³ Additionally, the screen capture reveals that, at the time the picture was created, his computer was connected to a Seagate removal media device called "Seagate Backup Plus."

³ The images show that KMEC accessed a KM-Logix page at the domain Just-Clause.com. An open source search revealed the domain just-clause.com is registered to KMEC, in addition to the domain farclause.com.

C. Contents of KMEC's Personal Email Account

33. During the course of this investigation, law enforcement obtained a search warrant for KMEC's email. During a review of the email return, law enforcement reviewed emails that suggest KMEC is currently in the process of applying for and interviewing for similar government contracting roles at other CDCs, including, but not limited to, Northrup Grumman, Lockheed Martin, Accenture, Raytheon, and QuantaDyn Corporation. In these emails, KMEC indicates that he left ADSI because it "is closing down its operations in Herndon, merging with another unit in Texas." In an undated draft email, KMEC indicates that he "was even thinking about selling my site because I'm currently out of funds." KMEC has also exchanged emails with a realtor and has expressed interest in selling the SUBJECT PREMISES at some point in the spring of 2019. Law enforcement have also observed during surveillance of KMEC that he is interviewing for other jobs.

34. In two different documents located in KMEC's Google Drive folder, one named "INTERVIEW" and the other "VA_UNEM," KMEC appears to outline his reasons for resigning from ADSI, both include a number of grievances that KMEC had with the company prior to his departure. In the "INTERVIEW" document, KMEC indicates that he "didn't see the future with this company. Not a job that I signed up for. . . . Quit to be able to focus on my next career move." In the "VA_UNEM" document, KMEC says, among many other things, that he was "effectively forced out after they searched my vehicle. all [sic] contracts on the drive were used as part of my duties that that I was assigned to. everyone [sic] is using UBS key, including Greg, who brought many of the documents from BAE."

D. There is Probable Cause to Believe that the Data on the Seagate Drive Contains ADSI Trade Secrets

i. *Data on the Seagate Drive Includes Financial, Business, Scientific, Technical, Economic or Engineering Information*

35. ADSI subject matter experts continue to examine the data that ADSI was able to copy from KMEC's Seagate drive. A partial review of information reveals that the ADSI information copied from the Seagate drive contains proprietary ADSI information and trade secrets, including past contracts, bids, pricing, competition strategies, and technical schematics for customers in the commercial, defense, and other government sectors. ADSI personnel estimated that approximately 50% of the files in the directory titled "Airbus" met the definition of a "trade secret." For example, the documents included information related to helicopters schematics, technical computer-aided designed drawings, and information regarding various technical instruments.

36. Other files copied from the Seagate drive related to ADSI proposals to the U.S. Government, including an ADSI proposal to the U.S. Army for the Light Utility Helicopter (LUH). Included in this data were technical diagrams, schematics, and contractual data. The data also contained information about two sensitive design features of the LUH: the communications system and the gearbox, which allow two engines to power a single gearbox. This design is proprietary to ADSI and not publicly known. According to ADSI, competitors had not yet been able to recreate the gearbox or the engine inlet barrier filter, which provides the LUH a "combat advantage" in high-dust or desert environments.

37. The LUH contract was run out of another ADSI office in Alabama and was finalized prior to KMEC's employment at ADSI; therefore, according to ADSI, there was no reason for KMEC to access the information or to possess a copy of it.

38. Many other files copied from the Seagate drive related to projects in which KMEC had no involvement or reason to access, and which predated KMEC's employment at ADSI. Moreover, according to KMEC's supervisor, there was no reason or legitimate business need for KMEC to download entire directories of information because KMEC was not an engineer.

39. The Seagate drive also included documents marked proprietary that belonged to BAH, KMEC's former employer, and ManTech International Corporation, KMEC's wife's current employer.

ii. *ADSI Took Extensive Measures to Keep Information Secret*

40. ADSI employs robust measures to protect trade secrets, including physical security measures, network security measures, and employee training. For example, to gain access to the third floor of the facility where KMEC worked, employees must use individually-issued badges at the access doors. ADSI personnel are instructed not to "piggyback" or "tailgate" behind other employees when going through these doors. ADSI uses surveillance cameras, locks, and alarms as additional physical security measures.

41. Once inside this secured space, employees need ADSI-issued credentials to logon to the computer network, which uses two-factor authentication. Additionally, ADSI's sensitive and/or proprietary information is accessible only to certain employees who have a need to know.

42. ADSI complies with the Department of Defense requirements for safeguarding defense information. ADSI IT personnel are able to monitor the network and detect intrusions before they occur. ADSI required its employees to take Information Assurance training, which includes training about cyber security awareness and information technology policies and procedures, at least twice a year.

43. The ADSI network also includes a banner message that prompts at login that states the following:

Warning! This is Airbus Group, Inc. information systems and by using this system you consent to and agree to the following:

- a. Any information accessed viewed received stored processed or transferred using this system may be monitored recorded and reviewed by system administrators and security personnel to ensure that use of this systems complies with all applicable laws regulations and Company policies;
- b. You understand that the Company is required by its Special Security Agreement to monitor all electronic communities between system users and Affiliates;
- c. If monitoring of this System reveals possible evidence of violation of criminal statutes this evidence and other related information including the identity of the user may be provided to law enforcement officials or Defense Security Service personnel;
- d. Use of this Information System contrary to law regulations or U.S. security policies or the policies plans and procures of the Company such as the Special Security Agreement the Implementation Procedures the Technology Security Plan or the Electronic Communications Plan (all of which are published on the Company's Command Media Library) are subjected to disciplinary action which may include termination of employment.

44. KMEC was required to sign an "Employee Agreement Regarding Protection of Company Assets" which restricted the "unauthorized disclose and use of [ADSI] proprietary information," and included the following language:

- a. I acknowledge that all files, documents notes, letters, email messages, memoranda, reports, records, data, sketches, drawings, models, laboratory notebooks, program listing, computer equipment and devices, computer programs and other written, photographic, and other tangible and intangible material containing Business Confidential Information [], whether created by me or others, that has or shall come into my custody or possession under the course of my employment, shall be and are the exclusive property of the Company. I will hold in strict confidence and will

not disclose, use, lecture upon, or publish any Business Confidential Information, except as such disclosure, use or publication may be required in connection with my work for the Company, and in compliance with Company policies I will obtain the Company's written approval before publishing or submitting for publication any material . . . that relates to my work as the Company and/or incorporates any Business Confidential Information. I agree that the obligations of this [paragraph] shall continue after termination of my employment with the Company.
...

- b. The term "Business Confidential Information" means any and all business confidential, proprietary, private, or secret knowledge, data, or information of the Airbus Group, whether or not in writing. By way of illustration, but not limitation, Business Confidential Information includes:
 - i. trade secrets, inventions, ideas, processes, formulas, source and object codes, data, programs, other works of authorship, know-how, improvements, discoveries, developments, designs and techniques. . . .
 - ii. information regarding plans for research, development, new product and services, marketing and selling, business plans, licenses, negotiations strategies and positions, projects, suppliers, customers, and prospective customers, including without limitation customer lists and contacts;
 - iii. personnel information, including information regarding the skills and compensation of other employees of Airbus Group;
 - iv. financial information, including projections, sales costs, profits, pricing methods, budgets and unpublished financial statements, and
 - v. any other information that derives value from not being generally known to the public or within the field in which Airbus Group competes.

45. In addition to the security measures mentioned above, ADSI also used exit interviews and emails to warn employees about potential security threats in an effort to protect the data.

46. KMEC worked as a Contracts Officer across multiple programs, which provided him with a greater degree of access to data on ADSI's network.

47. As soon as KMEC resigned from the company, ADSI notified building security that KMEC was no longer permitted to enter the building, and provided a photograph of KMEC so he could be easily identified. ADSI also circulated an email to all personnel informing them that KMEC was no longer an employee and reminded them that only current employees are permitted inside the building.

iii. ADSI Derived Economic Value from the Trade Secrets

48. ADSI personnel identified numerous documents copied from the Seagate drive that could have a severe economic impact on ADSI if the information were compromised. According to the company, the potential financial loss to ADSI due to the misappropriation of the data located on the Seagate drive would be significant.

49. The information copied from the Seagate drive included information that, according to ADSI, allows the company to win contracts and maintain a competitive edge against other CDCs. For example, one of the directories copied from the Seagate drive contained information about an ADSI proposal for an air tanker contract, which ADSI competed for against another company. The contract was valued at \$40 billion and ADSI spent significant amounts of money to develop the contract proposal. Included in the air tanker documents on KMEC's Seagate drive was a document named "Section J Attachment 06 – Integrated Master Plan (IMP)," which ADSI described as a "key component" of the bid to the U.S. military. The document, which is marked "proprietary," outlines ADSI's execution plan and shows how they ran the program, including the project timeline and milestones.

50. Exposure of this information, as well as other trade secrets described above, would likely benefit the recipient and harm ADSI. For example, a competitor would benefit from the above-mentioned LUH and air tanker documents because it includes specifics regarding how the proposals were awarded to Airbus by the U.S. Government. Such information would give them an advantage when competing for similar or follow-up contracts.

E. KMEC's Personal Business and Possible Use of Trade Secrets to Injure ADSI and Benefit Himself

51. According to the farclause.com/KM-Logix website, KMEC's personal business offers a tool that extracts all clauses from a user's request for proposal ("RFP") or contract and performs a comprehensive analysis and compliance check against the estimated 2000 clauses and provisions contained in the Federal Acquisition Regulation ("FAR"), Defense Acquisition Regulation Supplement ("DFARS"), and other U.S. Government regulations. According to the website, the tool "[q]uickly locate[s] FAR clauses that may impact your proposal's price and/or increase the risk performance." Users can also conduct searches based on FAR titles, prescriptions, versions, subcontractor flow-down requirements, or full text of clauses and provisions. Farclause claims to be a cloud-based website that is hosted on a secure server. Access to and use of the Premium version of the website costs \$199 per month.

52. KMEC's personal business could benefit from access and use of ADSI's proprietary information. KMEC could use ADSI trade secrets—particularly the internal contracts and RFPs that contain clauses or flow-down requirements—to benefit his website and company.

53. According to ADSI subject matter experts, to verify and hone the accuracy of his tool, KMEC likely would need to test it against real-world contracting data. Additionally, developers of automated contracting software require significant quantities of raw data to create

or fine-tune their products or programs, data which they will pay significant amounts of money to obtain and use. The type of data contained on the Seagate drive, including ADSI trade secrets, could be used to test and improve his software.

54. Moreover, after conducting a forensic analysis of the information on the Seagate drive, ADSI IT personnel identified that the source data for at least some of the information used by KMEC's personal business software was property of ADSI. Specifically, while monitoring KMEC's computer usage, ADSI IT personnel observed that KMEC was actively working with files located on the Seagate drive that were also located in Farclause directories or titled as such from his work computer. They determined that Microsoft Access⁴ files that KMEC was using in connection with Farclause contained links that connected back to ADSI files located both on his Seagate drive and on the ADSI network. Examples of the Access file names found on the Seagate drive include "ALL AIRBUS CONTRACTS-FPDS_Backup," "ALL AIRBUS CONTRACTS," and "Cayman - MANT."

55. Based on the presence of ADSI contract information in database files that pertain to KMEC's personal business, and the fact that ADSI information and KMEC's personal business information were comingled on the Seagate drive, and the relevance of ADSI trade secrets to KMEC's personal business, there is probable cause to believe that KMEC intended to convert and converted ADSI trade secrets.

⁴ Microsoft Access is a database management tool that allows the user to open and collate multiple databases simultaneously. Based on a review of KMEC's Gmail, in the spring of 2017, he paid an individual who specializes in website development to "export or link an MS Access application into an SQL server," which is a relational database management system developed by Microsoft. Upon completion of this project, KMEC sent this individual an email confirming that he had destroyed all of the data that KMEC had previously uploaded to the server in connection with the work in accordance with their nondisclosure agreement.

F. KMEC's Cell-Site Location Data Placing him at the SUBJECT PREMISES

56. Based on an analysis of KMEC's cellular phone data (obtained from his cellphone provider pursuant to an electronic search and seizure warrant) for October 17, 2018, KMEC stopped at a daycare⁵ located in Ashburn, Virginia, after departing ADSI that day. KMEC arrived at the SUBJECT PREMISES later that day.⁶

57. Based on an analysis of KMEC's Google account (obtained pursuant to an electronic search and seizure warrant), KMEC logged into his email (maroskmec@gmail.com) from an IP address that resolved to Ashburn, Virginia over 100 times on October 16, 17, and 18, 2018. As of December 2018, KMEC continued to log into his Google account from Ashburn, Virginia.

G. There is Probable Cause to Believe that Evidence of KMEC's Criminal Activity is Located in the SUBJECT PREMISES

58. Public records searches and over 40 hours of FBI surveillance confirmed that, as recently as January 2, 2019, KMEC still resides at the SUBJECT PREMISES. Open source domain registration records for farclause.com reveal that the SUBJECT PREMISES is listed as the physical address of record for the domain farclause.com. An open source search reveals SUBJECT PREMISES is listed as the address for KM-Logix/Farclause; the address is also included in the company's Google reviews.

⁵ As recent as December 18, 2018, KMEC was observed at the same daycare in his Lexus SUV before returning to the SUBJECT PREMISES.

⁶ Aside from a geolocation data placing KMEC's cellular phone at his the SUBJECT PREMISES at 11:32 p.m. that evening, there is no further coverage after KMEC arrived at the SUBJECT PREMISES earlier in the day.

59. A review of Virtual Private Network (VPN) logs for KMEC provided by ADSI from November 1, 2017 through November 2, 2018, show that KMEC remotely accessed ADSI's network on approximately 15 different occasions.⁷ Of these instances, 7 accessed the network from IP locations in Ashburn, Virginia.

60. I have checked available databases and I can find no record that KMEC owns another property where the Seagate drive may be hidden or stored. An analyst with the U.S. Postal Service ("USPS") confirmed that, as recently as November 2018, KMEC does not own other properties within the United States. Further, the FBI has engaged in over 40 hours of surveillance of KMEC and he has not been observed at any other residence, storage facility, USPS post office box, or other location where he may store material and/or have access to a computing device for transferring information. Accordingly, there is probable cause to believe that the ADSI trade secrets and evidence that KMEC used ADSI trade secrets may be located in the SUBJECT PREMISES.

61. Based on my training and experience with trade secret theft and similar federal violations, I know that individuals who are involved in the illegal possession of misappropriated information often retain it at their residence. In this case, after ADSI confronted KMEC, he left his ADSI workplace for a little over 50 minutes in his Lexus SUV. The SUBJECT PREMISES is approximately 15 minutes away from the ADSI office. It is reasonable to believe that KMEC traveled to the SUBJECT PREMISES during the 50 minutes he left ADSI to drop off the Seagate drive. Even if this is not the case, there is probable cause to believe KMEC took the Seagate drive to the SUBJECT PREMISES when he returned home at end of the day.

⁷ KMEC's supervisor confirmed that KMEC was allowed to work from home approximately five times in the previous year.

62. Based on my training and experience, and based on KMEC's level of education and years of experience in this field, and based on the fact that KMEC's Google logins show that he was using a Windows computer from an IP address in Ashburn, Virginia, I believe KMEC has at least one home computer that he uses to access the large amount of data stored on the Seagate drive. Although ADSI staff know that he spent a significant amount of time at ADSI working on his company and its website,⁸ it is likely that he continued to work on this after hours from the SUBJECT PREMISES. This would explain why KMEC would remove the device from his work laptop when he left work every evening. Further, even an individual without KMEC's technical skills would still be able to transfer the misappropriated information from a hard drive to a home computer.⁹

TECHNICAL TERMS

63. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service

⁸ Based upon a review of KMEC's Gmail account, KMEC sent multiple emails to multiple people regarding KM-Logix/Farclause during work hours, occasionally on the same day KMEC emailed his supervisor to notify him that he would not be coming in due to an illness.

⁹ Based on a review of information provided by Google pursuant to the search warrant, KMEC has logged into his account from a Windows PC, Apple iPad, and Apple iPhone 9 as recently as December 2018.

providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

64. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, including the Seagate drive discussed above and mobile phones, including smart phones. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

65. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

66. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES as further described in ATTACHMENT A because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when,

where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and

have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to copy information from a company's system, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

67. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.


68. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

69. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.


CONCLUSION

70. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,


Austin I. Price
Special Agent
Federal Bureau of Investigation

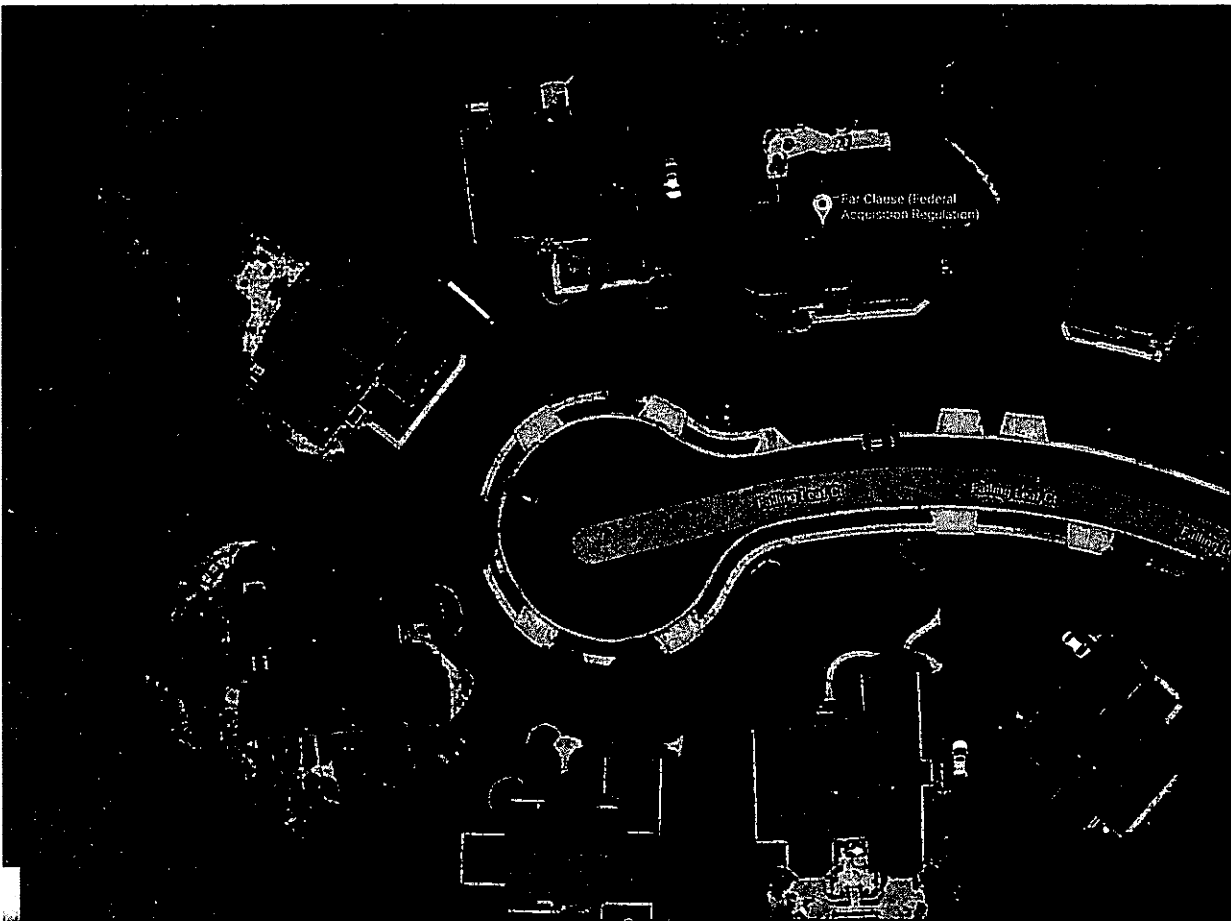
Subscribed and sworn to before me
on this 16th day of January, 2019.

 /s/ 
John F. Anderson

United States Magistrate Judge
Hon. John F. Anderson
United States Magistrate Judge

ATTACHMENT A

The property to be searched is the residence located at 42838 Falling Leaf Court, Ashburn, Virginia 20148. The SUBJECT PREMISES is further depicted in the below photographs and is described as a large single family home on Falling Leaf Court with the numbers "42838" clearly affixed to the home/mailbox and visible from the street. The vehicle has been observed at the SUBJECT PREMISES as recently as January 2, 2019. In addition, the search shall be extended to any locked safe or container within the SUBJECT PREMISES. It shall also be extended to Maros Kmec's Lexus SUV, which he drove to and from work on October 17, 2018.



Google Maps overhead image of 42838 Falling Leaf Court, Ashburn, Virginia 20148

ATTACHMENT B

The following is a list of property to be seized from within the premises known as 42838 Falling Leaf Court, Ashburn, Virginia 20148, a Lexus SUV, and any safes, lockers and closed containers therein, which constitutes evidence, fruits or instrumentalities of violations of the following federal statutes: Title 18, United States Code, Section 1832 (Theft of Trade Secrets); Title 18, United States Code, Section 2314 (Interstate Transportation of Stolen Property); Title 18, United States Code, Section 1343 (Wire Fraud); Title 18, United States Code, Section 2 (Aiding and Abetting the foregoing offenses); and Title 18, United States Code, Section 371 (Conspiracy to commit the foregoing offenses).

- a) Any and all financial, business, scientific, technical, economic and engineering information, of any form or type, relating to ADSI's or another company's proprietary information or trade secrets, which appears to be legally or equitably owned by, or licensed to, ADSI or another company, including, but not limited, to patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs and codes, and contracts, stored in any manner such as physically, electronically, graphically, photographically or in writing.
- b) Any other confidential information related to ADSI's and any other company's proprietary information or trade secrets, including but not limited to business records which reflect the source, development, marketing or sale of proprietary information or trade secret data, including, but not limited to, customer lists, customer files, customer correspondence, customer billing records, pick-up and delivery tickets, employee and drivers records, insurance

records, financial records, invoices, contracts, bank records, investment records, canceled checks, drafts, money orders, cash, memoranda, correspondence, handwritten notes, notebooks, telephone directories, address listings, and calendars.

- c) Any and all records of measures taken to keep secret proprietary information or trade secret data, including but not limited to exit interviews, confidentiality agreements (e.g., with employees, vendors, customers and competitors), non-compete agreements, employee contracts, employee handbooks or manuals, non-disclosure and unauthorized use warnings.
- d) Any and all records of legal or equitable ownership of, or license in, proprietary information or trade secret data by ADSI or any other company, and use or intended use of proprietary or trade secret data.
- e) Any and all records or other materials relating to the theft, misappropriation, unauthorized conversion, receipt, purchase or possession by any person[s] or entit[ies] other than ADSI of the proprietary information or trade secret data including, but not limited to, documents relating to the formation of corporate entities, business plans and venture capital proposals.
- f) Any and all records of employment offers and/or negotiation of employment terms by such person[s] or entit[ies].
- g) Any communications between such person[s] or entit[ies] and parties other than ADSI relating to proprietary information or trade secret data.
- h) Resource or reference materials relating to such financial, business, scientific, technical, economic and engineering information, including, but not limited

to, technical manuals, trade association documents, treatises.

- i) Conversations, whether through text message or other applications, where Maros Kmec discusses ADSI's proprietary information or trade secret data with other individuals.
- j) Computers and associated devices which could be used to transmit or store any of the above described financial, business, scientific, technical, economic and engineering information and books and records, including but not limited to:

- Computer Hardware – all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data, including any data-processing devices (such as central processing units, memory typewriters, self-contained “laptop” or “notebook” computers, mobile phones, including “smart” phones, tablets, and server computers), internal and peripheral storage devices (such as fixed disks, external hard disks/drives, including but not limited to, the Seagate external hard drive discussed in the affidavit, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices), peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers), related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling

devices, and electronic tone-generating devices), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks);

- Digital Storage Devices – any and all tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, including external hard drives, monitors, computer printers, modems, tape drives, thumb drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, tape systems and hard drive and other computer related operation equipment, in addition to computer photographs, Graphic Interchange formats and/or photographs, slides or other visual depictions of such Graphic Interchange format equipment which may be, or are used to send, receive, or store documents in an electronic format;
- Computer Software – digital information that can be interpreted by a computer and any of its related components to direct the way it works, stored in electronic, magnetic, optical, or other digital form, including but not limited to programs to run operating systems and applications (like word-processing, graphics, or spreadsheet programs, utilities, compilers, interpreters, and communications programs);
- Computer-related Documentation – written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, software, or other related items; and

- Computer Passwords and Other Data Security Devices – passwords (usually but not always a string of alpha-numeric characters) and other data security devices, including but not limited to encryption devices, chips, and circuit boards, programming code that creates “test” keys or “hot” keys which perform certain pre-set security functions when touched, software or code which encrypts, compresses, hides, or “booby-traps” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

Definitions

As used above, the terms “information,” “records,” “materials” and “documents” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including floppy diskettes, hard disks and external hard drives, ZIP disks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, mobile phones, including “smart phones,” and tablets, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).